AMENDMENTS TO THE SPECIFICATION:

Please amend the paragraph beginning on line 8 of page 1 as follows:

The present invention relates to an apparatus and a method for embedding information for tamper detection and detecting ~~tamper~~ tampering, and a recording medium having a program for carrying out the method recorded thereon. More specifically, the present invention relates to an apparatus for embedding authentication data for tamper detection in a digital image signal, extracting embedded data therefrom to detect any partial change in the digital image and localizing its position, a method carried out by the apparatus, and a recording medium having a program for carrying out the method recorded thereon.

Please amend the paragraph beginning on line 20 of page 1 as follows:

Recently, more and more information are available through the use of the Internet. Especially, WWW (World Wide Web) is being frequently used for transmitting and receiving information including images and audio. Under such a network environment opened for everyone, however, an indefinite number of people can copy digital information such as an image without difficulty. Further, the copied image can be easily edited or processed by image processing software available. Accordingly, there may be a case that a recipient of the digital image is not aware of any ~~tamper~~ tampering therewith that may have been made by a third party during the transmission.

Please amend the paragraph beginning on line 20 of page 4 as follows:

Further, with the conventional digital watermarking technique, specific information is embedded utilizing- high-frequency components which are normally insensible to human eyes. For this reason, if the digital image is subjected to irreversible image processing (compression and decompression) such as JPEG after being embedded with the information, such information is varied, making it impossible to extract the information correctly. That means that distinction is not possible between the ~~tamper~~ tampering intentionally made by an unauthorized person and the change unintentionally caused by the ordinary irreversible image processing.

Please amend the paragraph beginning on line 6 of page 5 as follows:

Still further, the high frequency components normally corresponds to an edge and texture part of an image. Accordingly, if the image is much composed of a monotonous part (image with little contrast variation), the information is not evenly embedded in the image (screen). As a result, a ~~tamper~~ tampering with such monotonous part may not be detected.

Please amend the paragraph beginning on line 14 of page 5 as follows:

Therefore, an object of the present invention is to provide an apparatus for embedding information for tamper detection and detecting ~~tamper~~ tampering that embeds specific information not only in high frequency components but in an entire image, i.e., in transform coefficients of relatively low frequency components, and later extracts the embedded information, a method carried out by such apparatus, and a recording medium having a program for carrying out the method recorded thereon. Therefore, it is possible to distinguish an intentional image tampering from a change unintentionally caused by irreversible image processing and further localize a tampered position.

Please amend the paragraph beginning on line 12 of page 26 as follows:

If the absolute value |Wi| is less than the set value T in step S702, the authentication data embedding portion 14 sets the transform coefficient Wi to a predetermined value +m or –m depending on a bit value of authentication data corresponding to the transform coefficient(step S703). Herein, the value m can be set at will as long as ~~being~~ it is not more than the set value T. The smaller the value m is, the better the deterioration in image quality becomes, but the less the protection against an external attack becomes. The larger the value m is, the better the protection against an external attack becomes, but the worse the deterioration in the image quality becomes due to the increase in amount of variation of transform coefficient. The value m thus may be appropriately set depending on the use of the apparatus and the level of the digital signal treated thereby. On the other hand, if the absolute value |Wi| is not less than the set value T in step S702, the authentication data embedding portion 14 sets, similarly to the key data embedding portion 13, q to a nearest even or odd integer depending on the bit value of authentication data corresponding to the transform coefficient (step S704). Here, q is assumed to be a value obtained by dividing a transform coefficient by quantization step size Q.

Please amend the paragraph beginning on line 8 of page 32 as follows:

The key data determination portion 22 is not an indispensable component to the tamper detecting apparatus 2. In the present invention, however, such determination for verifying the key data improves reliability of the tamper detecting apparatus 2 in detection of ~~tamper~~ a tampering with the digital image. The key data determination portion 22 is therefore preferably used in view of making the tamper detecting apparatus 2 more preferable in practical use.